UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,687	12/22/2000	Xun Wilson Huang	21816-04953	4655

758 7590 11/01/2005

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
ZHEN, LI B	
ART UNIT	**PAPER NUMBER**
2194	

DATE MAILED: 11/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/747,687	HUANG ET AL.	
	Examiner	Art Unit	
	Li B. Zhen	2194	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,16-32,36-52 and 56-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,16-32,36-52 and 56-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *05/09/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12,16-32,36-52 and 56-58 are pending in the application.

Response to Arguments

2. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-12, 16, 18, 21-32, 36, 38, 41-52, 56 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,647,422 to Wesinger et al. [hereinafter Wesinger] in view of U.S. Patent No. 6,055,637 to Hudson et al. [hereinafter Hudson].**

5. As to claim 1, Wesinger teaches the invention substantially as claimed including a computer-implemented method for virtualizing user privileges [an access rules database 113, including a Allow portion 115, a Deny portion 117; col. 4, lines 6 – 14] in a computer operating system including multiple virtual private servers [virtual hosts; col. 3, lines 49 – 60], the method comprising:

associating a user with a virtual private server [col. 3, lines 61 – 67] , the virtual private server comprising a plurality of actual processes [Child processes are created "on demand" as connection requests are received; col. 4, lines 12 – 29];

intercepting a system call, made by the user [daemon then uses a piece of code referred to herein as an INET Wrapper 710 to check on the local side of the connection and the remote side of the connection to determine, in accordance with the appropriate

Allow and Deny databases, whether the connection is to be allowed; col. 7, lines 20 – 27]; and

in response to the intercepted system call pertaining to the virtual private server associated with the user [All other rules must also be satisfied, regarding time of access, etc. If all the rules are satisfied, then the connection is allowed; col. 7, lines 54 – 63]:

allowing execution of the system call [Once the connection has been allowed, the daemon invokes HTTP server code 720 that operates in large part in a similar manner as conventional Web server. The HTTP server code 720 processes commands; col. 7, line 63 – col. 8, line 6].

6. Although Wesinger teaches the invention substantially as claimed, Wesinger does not teach designating the user as a virtual super-user, intercepting a system call, made by the user, for which actual user privileges are required and granting actual super-user privileges to the user.

However, Hudson teaches a resource access control method [col. 2, lines 3 – 12], designating the user as a virtual super-user [user is authorized to access one or more resources based on the role(s) assigned to the user; col. 3, lines 8 – 24], intercepting a system call, made by the user, for which actual user privileges are required [user identifier and password are passed to a trusted security authentication system 40; col. 2, line 50 – col. 3, line 8] and granting actual super-user privileges to the user [System 50 receives the user information and generates a temporary user credential token 52, which contains information such as the user's identifier authentication information, the user's role(s), and the user's access list, col. 2, line 67 – col. 3, line 8; Roles may include, for example, System Analyst I, Financial Advisor, Supervisor, Test Engineer, System Administrator, etc; col. 3, lines 8 – 28].

7. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teaching of designating the user as a virtual super-user, intercepting a system call, made by the user, for which actual user privileges are required and granting actual super-user privileges to the user as taught by Hudson to the invention of Wesinger because this provides role-based access control for

resources [col. 1, lines 51 – 56 of Hudson] and dynamically grants temporary access permission [col. 4, lines 10 – 15 of Hudson].

8. As to claim 2, Wesinger as modified teaches withdrawing the actual super-user privileges from the user after execution of the system call [When user 90 logs off from application program 94 at the end of the session, application program 94 terminates the session, and security package 96 deletes the temporary user credential token and also terminates the temporary access permission; col. 5, line 64 – col. 6, line 11 of Hudson].

9. As to claim 3, Wesinger as modified teaches assigning a virtual super-user identifier to the user [user identifier; col. 2, lines 50 – 67 of Hudson].

10. As to claim 4, Wesinger as modified teaches the virtual super-user identifier comprises a super-user identifier [Subject information are information on active entities or subjects, such as users; col. 3, lines 25 – 30 of Hudson] and an indication of the virtual private server [Each subject is preferably identified by a unique identifier; col. 3, lines 32 – 49 of Hudson].

11. As to claim 5, Wesinger as modified teaches assigning a user identifier to the user [user identifier; col. 2, lines 50 – 67 of Hudson] and storing the user identifier [Subject information are information on active entities or subjects, such as users; col. 3, lines 25 – 30 of Hudson] and an indication of the virtual private server of the user [Each subject is preferably identified by a unique identifier; col. 3, lines 32 – 49 of Hudson] in a virtual super-user list [a list of roles that are permitted to access the resource and the degree of access authorized for each role; col. 4, lines 28 – 49 of Hudson].

12. As to claim 6, Wesinger as modified teaches assigning a super-user identifier to the user [user identifier; col. 2, lines 50 – 67 of Hudson].

13. As to claim 7, Wesinger as modified teaches the intercepted system call comprises a system call for accessing a file [Each virtual host has a separate configuration sub-file, col. 3, lines 48 – 60 of Wesinger; configuration file C1, C2, etc., may have an access rules database 113, including a Allow portion 115, a Deny portion 117, col. 4, lines 6 – 11 of Wesinger].

14. As to claim 8, Wesinger as modified teaches the intercepted system call pertains to the virtual private server associated with the user when the file to be accessed is associated with the virtual private server [col. 5, lines 31 – 50 of Wesinger].

15. As to claim 9, Wesinger as modified teaches terminating a process [user 90 logs off from application program 94 at the end of the session, application program 94 terminates the session, and security package 96 deletes the temporary user credential token and also terminates the temporary access permission; col. 5, line 64 – col. 6, line 11 of Hudson].

16. As to claim 10, Wesinger as modified teaches the intercepted system call pertains to the virtual private server associated with the user [col. 3, lines 32 – 49 of Hudson] when the process to be terminated is associated with the virtual private server [col. 5, line 64 – col. 6, line 11 of Hudson].

17. As to claim 11, Wesinger as modified teaches identifying each process associated with the virtual private server [col. 3, lines 32 – 49 of Hudson], and terminating each identified process [temporary credential token is deleted when the session is terminated; col. 2, lines 20 – 25 and col. 5, line 64 – col. 6, line 11 of Hudson].

18. As to claim 12, Wesinger as modified teaches a data structure stores associations between processes and virtual private servers, and identifying each

process by its association with the virtual private server in the data structure [col. 3, lines 48 – 60 of Wesinger].

19. As to claim 16, Wesinger as modified teaches responsive to the intercepted system call not pertaining to the virtual private server associated with the user, disallowing execution of the system call [If the remote host is found in the Deny database, then the connection is denied; col. 7, lines 54 – 63 of Wesinger].

20. As to claim 18, Wesinger as modified teaches allowing comprises: executing the system call [col. 7, line 63 – col. 8, line 6 of Wesinger].

21. As to claims 21-32, 36 and 38, these are product claims that correspond to method claims 1-12, 16 and 18; note the rejections to claims 1-12, 16 and 18 above, which also meet these product claims.

22. As to claims 41-52, 56 and 58, these are system claims that correspond to method claims 1-12, 16 and 18; note the rejections to claims 1-12, 16 and 18 above, which also meet these systems claims.

23. **Claims 17, 19, 20, 37, 39, 40 and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesinger and Hudson further in view of U.S. Patent NO. 6,658,571 to O'Brien [cited in previous office action].**

24. As to claim 17, Wesinger as modified does not teach disallowing execution of a system call for inserting a module into an operating system kernel.

However, O'Brien teaches responsive to the intercepted system call comprising a system call for inserting a module [malicious software] into an operating system kernel, disallowing execution of the system call [each security module 105 "wraps" one or more applications 107 in the sense that applications 107 cannot access computing resources

106 for which they are unauthorized in the event that an application 107 executes malicious software; col. 3, lines 39 – 56].

25. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to disallow the execution of a system call for inserting a module into an operating system kernel as taught by O'Brien to the invention of Wesinger as modified by Hudson because this prevents malicious software from damaging computing resources that user is not normally allowed to access [col. 4, lines 33 – 37 of O'Brien].

26. As to claim 19, Wesinger as modified teaches loading a system call wrapper [Security modules 105 are kernel-loadable modules that make and enforce application-specific or resource-specific policy decisions for applications 107; col. 3, lines 38 – 56 of O'Brien], saving a pointer to the system call [each entry includes the following fields: a pointer to the original system call handler within the operating system; col. 5, lines 27 – 46 of O'Brien] and replacing the pointer to the system call with a pointer to the system call wrapper, such that the system call wrapper is executed when the system call is invoked [for each system call being wrapped, security master 103 redirects each pointer from the standard handler within the operating system to a corresponding system call wrapper within security master 103; col. 5, lines 27 – 46 of O'Brien].

27. As to claim 20, Wesinger as modified teaches the pointer to the first system call comprises a system call vector [Conventional operating systems include a system call table (ST) that contains pointers to handlers for the various system calls; col. 5, lines 28 – 46 of O'Brien].

28. As to claims 39 and 40, they are similar in scope to claims 19 and 20; therefore, claims 39 and 40 are rejected for the same reasons as claims 19 and 20 above.

29. As to claims 37 and 57, they are similar in scope to claim 17; therefore, claims 37 and 57 are rejected for the same reasons as claim 17 above.

Conclusion

30. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,374,292 to Srivastava et al. teaches access control system with rules that govern the granting of user level services for a domain.

U.S. Patent No. 6,484,173 to O'Hare et al. teaches controlling access to a data storage device includes defining a plurality of groups that access the data storage device.

31. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

32. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Li B. Zhen whose telephone number is (571) 272-3768. The examiner can normally be reached on Mon - Fri, 8:30am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Thomson can be reached on 571-272-3718. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Li B. Zhen
Examiner
Art Unit 2194

lbz

W. Thomson
TC 2100
SPE 2194